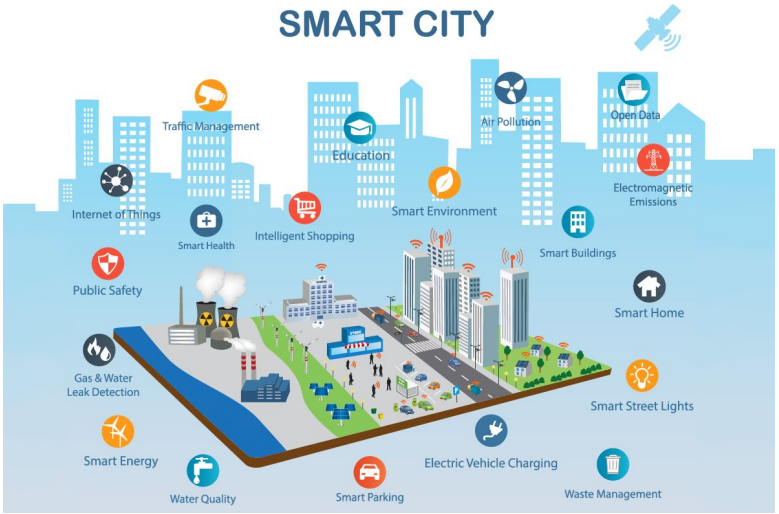
Smart Cities: Convenience or Chaos?

William Faircloth

What is a smart city?

- Smart cities leverage modern digital technologies like sensors, cameras, and data networks to manage its services more efficiently.
- Some key examples of smart city infrastructure:
  - Smart Traffic: Lights that adjust to real-time traffic
  - Smart Grids: Energy systems that reduce waste
  - Public Safety: Connected cameras and emergency response
  - Smart Utilities: Meters that track water and electricity use
- Smart cities rely on extensive data collection and analysis to work well.



What are the risks?

- While smart cities are an incredible technological feet, their convenience comes with risk that must be addressed.
- A single attack of the interconnected system can have severe kinetic consequences.
- Some examples of key threats include:
  - Critical Infrastructure: Hacking traffic lights (gridlock), the power grid (blackouts), or water systems.
  - Massive Data Breaches: Stealing the personal data of all citizens at once.
  - Service Disruption: Ransomware attacks that shut down city services (like the 2018 Atlanta attack).

Problem 1 — Privacy

- **Smart cities run on data.** To keep up with the data demands required for a connected city, surveillance *must* increase.
- This creates a conflict of **Efficiency** vs **Surveillance**
  - Smart traffic lights *need* to see the traffic.
  - Smart grids *need* to know your energy habits.
  - Predictive policing *needs* to track locations and people.
- The consequences of a smart city are constant, passive monitoring.
  - Facial recognition cameras, license plate readers, public Wi-Fi tracking, and smart meters create a detailed profile of your life.

How does this affect me?

- Examples of the privacy violations required to maintain a smart city can be seen here in Norfolk, Virginia.
- The Norfolk Police Department uses a technology called **Flock Safety cameras**.
- These are **Automated License Plate Readers (ALPRs)** that photograph every passing car, logging your license plate, vehicle, and the exact time and location.
- This system tracks all citizens, creating a searchable, 30-day database of your daily movements, which has led to federal lawsuits arguing this is **warrantless mass surveillance**.

Norfolk VA PD

Transparency Portal

Last Updated: Wed Nov 26 2025

Overview

The Norfolk Police Department (NPD) uses Flock Safety technology to capture objective evidence without compromising on individual privacy. NPD utilizes retroactive searches to solve crimes after they've occurred. Additionally, NPD utilizes real time alerting of hotlist vehicles to capture suspected criminals. In an effort to ensure proper usage and guardrails are in place, they have made the below policies and usage statistics available to the public.

Policies

What's Detected
License Plates, Vehicles

What's Not Detected
Facial Recognition, People, Gender, Race

Acceptable Use Policy
Data is used for law enforcement purposes only. Data is owned by NPD and is never sold to third parties.

Prohibited Uses
Any purpose other than law enforcement, usage based solely on a protected class (i.e. race, sex, religion), personal use, interference with any individual engaged in a lawful activity including lawfully protected speech.

Access Policy

Usage

Data Retention (In Days)
21 days

Number of Owned Cameras Operated by NPD
176

Hotlists Alerted On
NCMEC Amber Alert, NCIC - VSP

Vehicles Detected in the Last 30 Days
886,361

Hotlist Hits in the Last 30 Days
14,277

Searches in the Last 30 Days

Problem 2 — Ethics & Social Equity

Algorithmic Bias

- The AI algorithms that smart cities rely on are trained with human data, which is intrinsically biased.
- Algorithms designed for “predictive policing” are trained on historical arrest data, which can target and over-policy certain neighborhoods, demographics, and marginalized communities.

The Digital Divide & Accountability

- If essential services and utilities go exclusively digital, residents without reliable internet access or smartphones will be left behind.
- This also raises a key ethical question: If an algorithm makes a mistake, who is held responsible? The city, the AI, or the private tech vendor?

What do we do now?

- Given the severe ethical considerations, a nuanced solution that combines technical and social policy together.
- **Technical Solution**: Implement Network Segmentation so a compromise of a single unit of a smart city does not cascade across the city-wide infrastructure.
- **Social & Policy Solution**: Citizens must demand transparency and clear policies for surveillance technology like Flock, and citizens must have a say in how their data is used.

References

American Civil Liberties Union. (2022, February 15). *Automatic License Plate Readers*. American Civil Liberties Union. https://www.aclu.org/issues/privacy-technology/location-tracking/automatic-license-plate-readers

Flock Safety. (2025, November 26). *Norfolk VA PD Transparency Portal*. Flock Safety. Retrieved November 26, 2025, from https://transparency.flocksafety.com/norfolk-va-pd